Express Mail Label No.: EM 130482321 US
Date of Deposit: March 24, 2008

ATTORNEY'S DOCKET NO: **E0295.70066US00**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Steven M. Blumenau et al.
Serial No:	09/107,618
Filed:	June 30, 1998
For:	METHOD AND APPARATUS FOR PROVIDING DATA MANAGEMENT FOR A STORAGE SYSTEM COUPLED TO A NETWORK
Confirmation No.:	8313
Examiner:	Strange, Aaron N
Art Unit:	2153

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Attn: Board of Patent Appeals and Interferences

Sir:

REPLY BRIEF PURSUANT TO 37 C.F.R. §41.41

Richard F. Giunta
Reg. No. 36,149
Wolf, Greenfield & Sacks, P.C.
600 Atlantic Avenue
Boston, MA 02210
(617) 720-3500

Attorneys for Appellants

REPLY TO EXAMINER'S ANSWER

In response to the Examiner's Answer dated January 22, 2008, Appellant provides the following Reply Brief filed under 37 C.F.R. § 41.41. A Request for Oral Hearing is also being submitted herewith under a separate paper, as required under 37 C.F.R. § 41.47, along with a check for the fee required under 37 C.F.R. § 41.20(b)(3). No fee for this Reply Brief is believed to be due. However, if there is a fee occasioned by this submission, including any extension fee, please charge to Deposit Account No. 23/2825.

I. The Examiner's Remarks Seek to Improperly Shift the Burden

Without an assertion that Ericson teaches an untrusted environment, there is no reason to modify Ericson with the authentication techniques of Yu. The Examiner's Answer concedes that Ericson "does not even contain a single instance of the words 'trust' or 'trusted environment'" (Examiner's Answer, Page 9). That should end the inquiry, as without a teaching that the system described in Ericson could be in an untrusted environment, there is no reason to modify Ericson with the authentication techniques of Yu. However, the Examiner misapprehends his burden in establishing a *prima facie* case of obviousness, and argues essentially that Applicant has not *proven* that Ericson discloses only trusted environments.

While Appellant believes that Ericson discloses a trusted environment for all of the reasons discussed in the Appeal Brief and below, that "debate" about Ericson must be considered in the context of the appropriate burden, which rests with the Examiner. It is not Appellant's burden to prove beyond a shadow of a doubt that Ericson's system could not be used in an untrusted environment, but rather it is the Examiner's burden to find some teaching to use the Ericson system in an untrusted environment (i.e., an environment vulnerable to identify spoofing from bad actors) so that the system would benefit from adding authentication techniques. The Examiner has not and cannot point to any such teaching, and therefore cannot meet the burden necessary in establishing a *prima facie* case.

As discussed above, the Examiner agrees that Ericson mentions nothing about whether the environment is trusted or untrusted. Appellant has provided evidence that SCSI is a limited and constrained protocol to show that it is more likely than not that the environment in Ericson is trusted, and that Ericson discloses nothing more than the state of the art at the time of the invention (i.e., storage devices accessed by local and known devices). Rather than producing evidence suggesting that Ericson is an untrusted environment, the Examiner instead argues that Appellant hasn't shown that Ericson is *necessarily* a trusted environment. Indeed, the Examiner's Answer asserts that Appellant's entire argument relies on the "inherent security of a SCSI environment," while the rejection of the claims is based on the so-called "Fibre Channel embodiment" (Examiner's Answer, page 11). However, even if it were true the SCSI embodiment could be entirely removed and replace with the "Fibre Channel embodiment," the Examiner still has the burden of showing that the mere reference to the Fibre Channel protocol somehow suggests that the Ericson system be used in an environment that would benefit from the authentication techniques of Yu, which the Examiner has failed to do.

Fibre Channel is a protocol that can be used in both trusted and untrusted environments so that the mention of Fibre Channel does not in any way indicate whether an environment is trusted or not. Indeed, the Examiner concedes that it is "undoubtedly true" that using the Fibre Channel protocol does not by itself convert a trusted environment to an untrusted environment," but argues that using Fibre Channel "does eliminate the inherent security found in a SCSI environment" (Examiner's Answer, page 11). Even if this were true and the alleged Fibre Channel embodiment was implemented without using SCSI and was therefore free from the "inherent security" of the SCSI embodiment, the Examiner still has not pointed to any teaching that the system of Ericson be used in an environment that would make modifying Ericson with additional security features such as the authentication techniques of Yu desriable. There are many ways of implementing a trusted network, including using the Fibre Channel protocol.

The Final Office Action and the Examiner's Answer cite Boggs in an effort to provide some suggestion of the desirability of adding additional security features to the system described in Ericson. In particular, the Examiner's Answer asserts that it is "well known in the art at the time of the invention that SCSI peripherals may be distributed over wide area network using ATM and Fibre Channel," referencing Boggs to support this assertion (Examiner's Answer, page 4). However, as discussed in detail in Appellant's Brief, Boggs teaches <u>nothing</u> of the sort.

Nowhere does Boggs in any way disclose or suggest that SCSI peripherals may be distributed over a wide area network using ATM and Fibre Channel. In fact, in every instance where Boggs discusses peripherals (i.e., the disk arrays) it is in the context of a local and contained environment.

Specifically, Boggs describes the disk arrays in three parts of the disclosure. First, column 2, lines 21-23, in describing the system illustrated in FIG. 11, state "[f]urther, each processing system 1102, 1104, 1106, 1108 may access a plurality of disk arrays 1122, 1124, 1126, 1128 via a peripheral bus 1130 such as a SCSI bus." Second, column 2, lines 39-41, in describing the system in FIG. 12, similarly state "[f]urther, each processing system 1202, 1204, 1206, 1208 may access a plurality of disk arrays 1222, 1224, 1226, 1228, via, for example, a SCSI bus 1230." It should be appreciated that the local area network (LAN) clients <u>do not have access to the disk arrays</u> (they are not even connected). Finally, the only other mention of how the disk arrays are connected is described in column 3, lines 52-63, which state:

> FIG. 1 illustrates a universal ATM interconnect system 100 according to the present invention. In FIG. 1, an enhanced ATM switch 180 according to the present invention is connected to a plurality of processing systems or CPUs 102, 104, 106, 108. LAN operations between clients 110 and the processing system or CPUs 102, 104, 106, 108 are routed by the switch 180. Node to node messages between processing systems or CPUs 102-108 are handled by the switch 180. Input/output operations between the processing system or CPUs 102-108 and a plurality of disk arrays 122, 124, 126 are handled also by the ATM switch 180.

Just as illustrated in FIGS. 11 and 12, the CPUs are the <u>only devices</u> that are described as having access to the disk arrays. Nowhere does it describe the disk arrays (or any other peripherals) as being distributed over a WAN, or capable of being accessed over a distributed network. To the contrary, in the excerpt above, Boggs makes an explicit distinction between LAN operations and I/O operations between the CPUs and the disk arrays. Accordingly, not only does Boggs not support the assertion that it is "well known in the art at the time of the invention that SCSI peripherals may be distributed over wide area network using ATM and Fibre Channel," it suggests the contrary by showing only local and constrained access to disk arrays.

While Boggs discloses that ATM switches may be used to implement WANs, MANs and LANs, it nowhere discloses or suggests distributing or providing access to the disk arrays over such networks. Boggs merely states that ATM can also be used as a peripheral communications mechanism. That is, ATM is not being used to connect the disk arrays to the LAN (or WAN for that matter). Boggs nowhere teaches this. Rather, ATM is used as a peripheral interface so that the CPU's can perform I/O operations with the disk arrays. No other network access to the disk arrays is disclosed or suggested. The citations in Boggs that the Final Office Action and the Examiner's Answer allege disclose distributing SCSI peripherals over a WAN simply do not describe anything of the sort. Indeed, in each instance where disk arrays are shown or described, they are shown as being accessed solely by the CPUs to which they are locally (e.g., peripherally connected). Not even LAN clients (e.g., LAN clients 110) are described as capable of accessing the disk arrays. Accordingly, just as in Ericson, Boggs would not need additional security measures because the only devices accessing the disk arrays are the local CPUs.

The state of the art in the area of storage devices at the time of the invention was local access by trusted devices (e.g., devices that were known and attached by an administrator). Both Ericson and Boggs confirm this. That the CPUs in Boggs can both communicate with LAN clients 110 and access the disk arrays, does not mean that the LAN clients can access the disk arrays. In fact, as discussed above, Boggs specifically differentiates the two types of communications, describing only the CPUs as performing I/O operations with the disk arrays. Boggs discloses nothing more than the state of the art described above – local access by trusted devices. Boggs in no way supports the assertion that it was well known in the art to distribute storage devices over a WAN, and therefore in no way supports the assertion that one of ordinary skill in the art would have been motivated to modify Ericson with the authentication techniques of Yu, which would be entirely unnecessary and serve only to complicate the design. The Examiner has failed to produce any reference that shows networked storage devices connected over a network such that it would be vulnerable to spoofing and thus benefit from additional security. Thus, the Examiner has failed to establish a *prima facie* case of obviousness, and the rejections under 35 U.S.C. §103 should be reversed.

II. The Examiner Selects Only the Teachings in Ericson that are Perceived to be Helpful While Ignoring Those That Teach Away From The Present Invention

While the Examiner's failure to meet his burden is sufficient to end the inquiry, Applicant respectfully points out that the Examiner's so-called "Fibre Channel embodiment" is an impermissible picking and choosing of disclosure from Ericson, rather than reading Ericson as a whole. As discussed in detail in the Appeal Brief, Ericson is directed to controlling access to a target device 102 (e.g., a disk array) by initiators 100 interconnected by a small computer system interface bus ("SCSI bus") 104, wherein the network devices are preconfigured in accordance with the SCSI specification. (Col. 3, lines 48-56). FIG. 1 of Ericson is reproduced below.

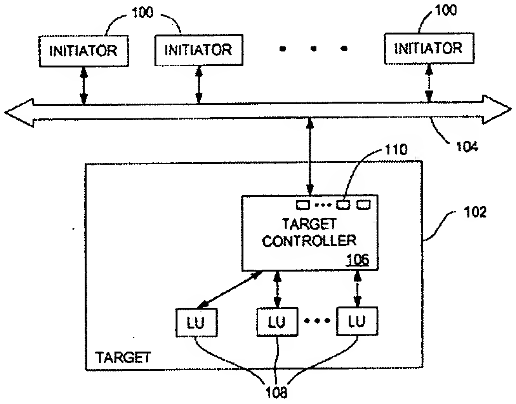

FIG. 1

The initiators 100 request access to the target 102 by directing an access message to the target 102 via the SCSI bus 104, the message including the initiator identifier, a target identifier and a portion of the target device 102 to be accessed (i.e., the logical unit 108). (Col. 3, lines 56-61). Access to the target device is controlled by a look-up structure preconfigured by a system operator who assigns selected logical units 108 in the target 102 to each of the initiators 100. This local SCSI environment, referred to hereinafter as the "SCSI embodiment," is the <u>only</u> environment in which Ericson describes authorization techniques.

The Examiner's Answer makes reference to a so-called "Fibre Channel embodiment," that the Examiner alleges is relied upon to reject the appealed claims. However, a mere two sentences in the entirety of Ericson allude to this so-called "Fibre Channel embodiment." The first reference is in the "BACKGROUND OF THE INVENTION" and states that network devices may be connected with conventional interconnection subsystems such as, for example, "a small computer interface parallel interconnect bus ("SCSI bus"), a SCSI Fibre Channel bus, or an Ethernet based local area network" (column 1, lines 12-16). The other reference is in the "DESCRIPTION OF ILLUSTRATIVE EMBODIMENTS" and states that other communications protocols may be used, for example, "conventionally known peripheral connect interface ("PCI") and Fibre Channel protocols" (column 6, lines 4-6). No description is given as to how Fibre Channel would be implemented, and nothing suggests that the resulting environment for such a "Fibre Channel embodiment" would differ in any way from the SCSI embodiment that is described in the entirety of the Ericson disclosure, excepting these two sentences.

The Examiner's Answer asserts that "Appellants' entire argument rests on the inherent security of a SCSI environment, which was not relied upon in rejecting the appealed claims. Since the prior art combination used to reject the appealed claims uses the Fibre Channel protocol, this inherent security is not present..." (Emphasis in original). Appellant respectfully asserts that the above quote from the Examiner's Answer makes clear that the majority of the teachings in Ericson were ignored and the reference was not considered as a whole, which is impermissible. MPEP §2142.02(VI) is quite clear on this matter, stating a "prior art reference must be considered in its entirety, i.e., as a whole, including portions that would lead away from the claimed invention."

The Federal Circuit and its predecessor court have repeatedly indicated that when performing an obviousness analysis under §103, each reference must be considered in its entirety to determine whether it fairly suggests that the invention as a whole is obvious. See e.g., Bausch & Lomb v. Barnes-Hind/Hydrocurve, 230 USPQ 416, 419 (Fed. Cir. 1986) ("it is impermissible within the framework of §103 to pick and choose from any one reference only so much of it as will support a given position to the exclusion of other parts necessary to the full appreciation of what such reference fairly suggests to one skilled in the art."); In re Dow Chemical Co., 5 USPQ 2d 1529, 1531-1532 (Fed. Cir. 1988) (when determining whether a suggestion for the claimed invention can be found in the prior art, "the full field of the invention must be considered; for the person or ordinary skill is charged with knowledge of the entire body of technical literature, including that which might lead away from the claimed invention … Evidence that supports, rather than negates, patentability must be fairly considered.") (emphasis added); W.L. Gore & Associates, Inc. v. Garlock, Inc., 220 USPQ 303, 311 (noting that the District Court erred in its §103 analysis "in considering the references in less than their entireties, i.e., in disregarding disclosures in the references that diverge from and teach away from the invention at hand."); In re Kuderna and Phillips, 165 USPQ 575, 578-579 (CCPA 1970) (stating that the issue of what would have been obvious to one of ordinary skill in the art must be made "in view of the *sum* of all the relevant teachings in the art, not in view of first one and then another of isolated teachings in the art."); In re Wesslau, 147 USPQ 391, 393 (CCPA 1965) (reversing the Board's decision and noting that if one were to follow the teachings of the prior art reference "in its entirety", he would be led away from the Applicants' invention).

As discussed above, the only system described in Ericson that teaches the limitations relied upon by the Examiner in rejecting the appealed claims is in the context of a local SCSI environment. Accordingly, not only is it improper for the Examiner to ignore nearly the entirety of the Ericson disclosure, it is inaccurate to assert that the system described using the SCSI environment was not relied upon in rejecting the appealed claims. Indeed, each portion of Ericson cited in the Final Office Action and the Examiner's Answer that allegedly disclose various limitations in the claims are found within the description of the SCSI embodiment. Thus, it is incorrect to say that the SCSI embodiment is not relied upon – it is wholly relied upon in rejecting the portions of the claims for which Ericson was applied. In fact, rejecting the claims based on the SCSI embodiment, suggests that the same SCSI system would be used in implementing the so-called "Fibre Channel embodiment." Otherwise, the Examiner would have nothing left with which to reject the claims.

The Final Office Action and the Examiner's Answer only rely on the "Fibre Channel embodiment" under the misguided sense that it supports an assertion that Ericson would benefit from the authentication techniques of Yu. In doing so, they conveniently ignore the vast majority of Ericson. The Examiner has *created* the so-called "Fibre Channel embodiment" and alleged that this hypothetical embodiment would have benefitted from the authentication techniques of Yu without any support for this allegation in the entirety of Ericson or elsewhere.

Indeed, the Examiner points to nothing in Ericson that would suggest that a Fibre Channel implementation would require any more security than the SCSI implementation.

The Examiner even concedes that implementing the Fibre Channel protocol does not by itself convert a trusted environment into an untrusted environment. However, the Examiner's Answer indicates that "implementation of the Fibre Channel protocol does eliminate the inherent security found in a SCSI environment." This is an entirely unsupported assertion. There is no evidence that implementing Ericson's techniques using the Fibre Channel protocol would eliminate the inherent security found in a SCSI environment, or otherwise transform the environment described in Ericson to an untrusted environment requiring additional security measures. In fact, when reading the reference as a whole, Ericson suggests just the opposite.

In particular, the first of the two references to Fibre Channel actually discloses a SCSI Fibre Channel Bus. That is, a SCSI bus implemented using Fibre Channel. The second reference indicates that "Fibre Channel protocols" may be used. One of the most common Fibre Channel protocols is the SCSI Fibre Channel protocol (FCP). SCSI FCP is the interface protocol of SCSI on Fibre Channel. That is, the SCSI FCP allows a designer to *implement SCSI on Fibre Channel*. Accordingly, the Ericson reference actually suggests that the hypothetical "Fibre Channel embodiment" would more likely than not be implemented using SCSI, irrespective of what protocol is used, and does not suggest a different environment that is untrusted.

Thus, using Fibre Channel does not necessarily eliminate the inherent security found in a SCSI environment as asserted in the Examiner's Answer, and nothing in Ericson suggests that doing so impacts the security of the disclosed SCSI environment. That is, when Ericson is read as a whole, it is more plausible that the alleged "Fibre Channel embodiment" (of which no details are provided) would be built on the SCSI system to which Ericson devotes his entire disclosure. To allege that the "Fibre Channel embodiment" is some new, different and untrusted environment is to completely divorce Fibre Channel from the entire rest of the Ericson disclosure, which is impermissible.

III. Conclusion

The Examiner's Answer concedes that Ericson does not disclose that its environment is untrusted, and also that the reference to using the Fibre Channel protocol does not mandate an untrusted environment. That should end the matter. There is simply no support in Ericson, Boggs or elsewhere that the Ericson system, which represents the state of the art in the area of storage devices at the time of the invention (i.e., local and trusted) has any need for the authentication techniques of Yu. For the reasons set forth in Appellant's Appeal Brief and for the foregoing reasons, the rejections of each of the claims is improper and should be reversed.

Respectfully submitted,

Steven M. Blumenau et al., Appellant

Richard F. Giunta, Reg. No. 36,149
WOLF, GREENFIELD & SACKS, P.C.
600 Atlantic Avenue
Boston, MA 02210
Tel: (617) 646-8000
Attorneys for Appellants

Attorney Docket No.: E0295.70066US00
Dated: March 24, 2008